CLAIMS

1. A method for authenticating a software entity comprising:

locating a signed authentication block in a memory of a computer system;

employing a cryptographic technique to verify that the signed authentication block is authentic;

computing an authentication value from an in-memory image of the software entity; and

comparing the computed authentication value with an authentication value stored in the authentication block to determine whether or not the in-memory image of the software entity is identical to an expected in-memory image for the software entity.

2. The method of claim 1 wherein locating a signed authentication block in the memory further includes one of:

locating the signed authentication block in contiguous memory locations within the in-memory image of the software entity;

locating the signed authentication block in contiguous memory locations within an authenticating software entity; and

locating the signed authentication block in contiguous memory locations at a previously established memory location;

locating fragments of the signed authentication block in a number of previously established memory locations and assembling the signed authentication block from the located fragments in a number of contiguous memory locations.

3. The method of claim 1 wherein locating a signed authentication block in the memory further includes:

locating the signed authentication block by computing one or more memory locations and extents according to a previously established process.

4. The method of claim 1 wherein locating a signed authentication block in the memory further includes:

locating fragments of the signed authentication block in a number of previously established memory locations and assembling the signed authentication block from the located fragments in a number of contiguous memory locations.

5. The method of claim 1 wherein employing a cryptographic technique to verify that the signed authentication block is authentic further includes:

validating the authentication block using a public key and checking that the format of the validated authentication block corresponds to an expected authentication block format.

6. The method of claim 1 wherein employing a cryptographic technique to verify that the signed authentication block is authentic further includes:

validating the authentication block using a public key and checking that values included in the authentication block are identical to expected values.

7. The method of claim 1 wherein computing an authentication value from the in-memory image of the software entity further includes:

computing a cryptographic hash value using a cryptographic hash function.

8. The method of claim 7 wherein the cryptographic hash value is computed over the entire in-memory image of the software entity.

9. The method of claim 7 wherein the cryptographic hash value is computed over one or more portions of the in-memory image of the software entity.

10. The method of claim 1 further including:

comparing an additional computed authentication value with an additional computed authentication value stored in the authentication block to determine whether or not the in-memory image of the software entity is identical to an expected in-memory image for the software entity.

11. The method of claim 1 further including:

comparing an additional authentication value stored in the authentication block with a value observed from the memory to determine whether or not the in-memory image of the software entity is identical to an expected in-memory image for the software entity.

12. The method of claim 11 wherein the additional computed value is one of:

a stacked return pointer value;

a passed argument; and

an address of a particular instruction.

13. The method of claim 1 wherein the software entity is one of:

a program or routine called by a calling program or routine;

a program or routine that calls a different program or routine;

a library routine;

a software module; and

a program that seeks to authenticate itself.

14. Computer instructions encoded in a computer readable medium for carrying out the method of claim 1.

15. A method for constructing an authentication block used to authenticate the in-memory image of a software entity, the method comprising:

determining a location for the authentication block;

preparing a clear text temporary copy of the authentication block to include a computed value that can be subsequently calculated by a program based on the in-memory image of the software entity;

signing the clear text temporary copy of the authentication block to produce a signed authentication block; and

copying the signed authentication block into code from which the authentication block is subsequently copied into the determined location.

16. The method of claim 15 wherein determining a location for the authentication block further includes:

determining a memory location in or near the in-memory image of the software entity that can be later determined by an authorizing program in order to access the signed authentication block.

17. The method of claim 15 wherein determining a location for the authentication block further includes:

determining a number of memory locations in or near the in-memory image of the software entity that can be later determined by an authorizing program in order to access portions of the signed authentication block and assemble the signed authentication block.

18. The method of claim 15 wherein determining a location for the authentication block further includes:

determining a memory location in or near the in-memory image of an authenticating software entity that can be later determined by an authorizing program in order to access the signed authentication block.

19. The method of claim 15 wherein determining a location for the authentication block further includes:

determining a number of memory locations in or near the in-memory image of an authenticating software entity that can be later determined by an authorizing program in order to access portions of the signed authentication block and assemble the signed authentication block.

20. The method of claim 15 wherein the computed value is a cryptographic hash value generated by a cryptographic hash function on the expected in-memory image of the software entity.

21. The method of claim 15 wherein the computed value is a cryptographic hash value generated by a cryptographic hash function on one or more portions of the expected in-memory image of the software entity.

22. The method of claim 15 wherein signing the clear text temporary copy of the authentication block to produce a signed authentication block further includes:

signing the clear text authentication block using a private key.

23. The method of claim 15 further including:

including an additional authentication value into the clear text authentication block.

24. The method of claim 23 wherein the additional authentication value is one of:

a return pointer value;

the memory address of a particular type of instruction;

a passed argument;

a size of a portion of the software entity from which the computed value is generated;

a memory address for the start of the in-memory image of the software entity; and

any value that can be computed from the memory at the time that the authentication block is accessed by an authenticating routine.

25. A software entity including an authentication block prepared by the method of claim 15.

26. An authentication block prepared by the method of claim 15 stored in a computer readable medium.